

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of:
Information associated with account identified as
arizonasewingworks@gmail.com that is within the
possession, custody, or control of Google, LLC

)
)
)
)
)
2:23-MJ-6240

APPLICATION FOR WARRANT BY TELEPHONE PURSUANT TO 18 U.S.C. § 2703

I, a federal law enforcement officer, request a warrant pursuant to Title 18, United States Code, Section 2703, and state under penalty of perjury that I have reason to believe that within the following data:

See Attachment A

There are now concealed or contained the items described below:

See Attachment B

The basis for the search is:

- Evidence of a crime;
- Contraband, fruits of crime, or other items illegally possessed;
- Property designed for use, intended for use, or used in committing a crime.

The search is related to a violation of:

Code section(s)
21 U.S.C. §§ 841

21 U.S.C. §§ 846
21 U.S.C. §§ 953

Offense Description
Possession with intent to distribute and distribute controlled substances
Conspiracy to distribute controlled substances
Exportation of controlled substances

The application is based on these facts:

See attached Affidavit, which is incorporated herein by reference.

/s/ Martina Doino

Applicant's signature

Martina Doino, HSI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

Hon. Maria A. Audero, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

This warrant applies to information associated with the SUBJECT ACCOUNT identified as arizonasewingworks@gmail.com that is within the possession, custody, or control of Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California 94043 regardless of where such information is stored, held, or maintained.

ATTACHMENT B

ITEMS TO BE SEIZED

I. SEARCH PROCEDURES

1. The warrant will be presented to personnel of Google, LLC (the "PROVIDER"), who will be directed to isolate the information described in Section II below.

2. To minimize any disruption of service to third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the information described in Section II below.

3. The PROVIDER's employees will provide in electronic form the exact duplicate of the information described in Section II below to the law enforcement personnel specified below in Section IV.

4. With respect to contents of wire and electronic communications produced by the PROVIDER (hereafter, "content records," see Section II.10.a. below), law enforcement agents and/or individuals assisting law enforcement and acting at their direction (the "search team") will examine such content records pursuant to search procedures specifically designed to identify items to be seized under this warrant. The search shall extract and seize only the specific items to be seized under this warrant (see Section III below). The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques. The review of the electronic data may

be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

6. The search team will complete its search of the content records as soon as is practicable but not to exceed 120 days from the date of receipt from the PROVIDER of the response to this warrant. The government will not search the content records beyond this 120-day period without first obtaining an extension of time order from the Court.

7. Once the search team has completed its review of the content records and created copies of the items seized pursuant to the warrant, the original production from the PROVIDER will be sealed -- and preserved by the search team for authenticity and chain of custody purposes -- until further order of the Court. Thereafter, the search team will not access the data from the sealed original production which fell outside the scope of the items to be seized absent further order of the Court.

8. The special procedures relating to digital data found in this warrant govern only the search of digital data pursuant to the authority conferred by this warrant and do not apply to any search of digital data pursuant to any other court order.

9. Pursuant to 18 U.S.C. § 2703(g) the presence of an agent is not required for service or execution of this warrant.

II. INFORMATION TO BE DISCLOSED BY THE PROVIDER

10. To the extent that the information described in Attachment A is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, including any information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for SUBJECT ACCOUNT listed in Attachment A:

a. All contents of all wire and electronic communications associated with the SUBJECT ACCOUNT, including:

i. All emails, communications, or messages of any kind associated with the SUBJECT ACCOUNT, including stored or preserved copies of messages sent to and from the account, draft messages, deleted messages, and messages maintained in trash or any other folders or tags or labels, as well as all header information associated with each email or message (including the actual IP addresses of the sender and recipients of the emails), and any related documents or attachments.

ii. All records or other information stored by subscriber(s) of the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, videos, notes, texts, links, user profiles, account settings, access logs, and files.

iii. All folders and files associated with the SUBJECT ACCOUNT, included stored or preserved copies of files sent to and from the account, the source and destination addresses associated with the file(s), date(s), and time(s) at which each file was sent, and any user-created organizational structure within the SUBJECT ACCOUNT, or any files or messages saved in the account as a "draft" or any other manner.

iv. All records pertaining to communications between the PROVIDER and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

v. All transactional information of all activity of the SUBJECT ACCOUNT described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting, and email "invites" sent or received via PROVIDER, and any contact lists.

vi. All search history and web history, including web clicks or "History Events," by the user(s) of the SUBJECT ACCOUNT.

vii. All records pertaining to communications between PROVIDER and any person regarding the SUBJECT ACCOUNT,

including contacts with support services and records of actions taken.

viii. All web browsing activities that are identifiable with the SUBJECT ACCOUNT.

ix. All other records of communications and messages of any kind made or received by the user(s), including all private and instant messages or "chats," however saved, and specifically including all attachments to any messages in their native format (for example, if a .zip file was sent to another user, the .zip file shall be provided).

x. All photos and videos uploaded from the SUBJECT ACCOUNT, all photos and videos uploaded by any user that have the user tagged in them, and all photos and videos commented on by the user, as well as any metadata associated therewith, including any EXIF data.

xi. All of the following information created and/or shared by, and associated with, the SUBJECT ACCOUNT; profile information; Location Data; status updates; videos, photographs, various images (including "avatars"), and other items shared and received; records of videos, photographs, various images, and other items shared by the SUBJECT ACCOUNT and saved by other users; friend lists, including persons identified as "Friends," and including the friends' user names and display names (including those of any deleted or removed friends); groups and networks of which the user is a member, including any identification numbers; items purchased; notifications and notification settings of any kind; and

information about the user's access and use of third-party applications or "apps" and content shared with other users.

xii. All search history and web history for the user of the SUBJECT ACCOUNT that PROVIDER have access.

xiii. A complete list of the SUBJECT ACCOUNT's contact list(s) and chat partners deleted and undeleted.

xiv. All open and unopened one-to-one chats, including chats sent in groups.

xv. Any links, Uniform Resource Locators ("URLs"), or other messages sent or received to from the SUBJECT ACCOUNT, whether to or from PROVIDER or other persons.

xvi. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, PROVIDER shall provide the salt value used to compute the stored password hash value, and any security questions and answers.

b. All other records and information, including:

i. All subscriber information, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), any alternate names, other account names or email addresses associated with the account, linked accounts, telephone numbers, physical addresses, and other identifying information regarding the subscriber, including any removed or changed names, email addresses, telephone numbers or physical addresses, the types of service utilized, account

status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, and including any changes made to any subscriber information or services, including specifically changes made to secondary email accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred, for the SUBJECT ACCOUNT, and any other account associated with the SUBJECT ACCOUNT, including by means of sharing a common secondary, recovery, or alternate email address(es) listed in subscriber records for the SUBJECT ACCOUNT or by means of sharing a common phone number or SMS number listed in subscriber records for the SUBJECT ACCOUNT, and any account that lists the SUBJECT ACCOUNT as a secondary, recovery, or alternate email address.

ii. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

iii. Any information showing the location of the user of the SUBJECT ACCOUNT, including while sending or receiving a message using the SUBJECT ACCOUNT or accessing or logged into the SUBJECT ACCOUNT.

iv. All user connection logs and transactional information of all activity relating to the SUBJECT ACCOUNT described above in Section II.10.a., including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, and locations, and including specifically the specific product name or service to which the connection was made.

III. INFORMATION TO BE SEIZED BY THE GOVERNMENT

11. For each SUBJECT ACCOUNT listed in Attachment A, the search team may seize:

All information described above in Section II.10.a. that constitutes evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841 (possession with intent to distribute and distribution of controlled substances) 846 (conspiracy to distributed controlled substances), and 953 (exportation of controlled substances) (the "SUBJECT OFFENSES"), from July 1, 2023 to the present, namely:

i. Information relating to who created, accessed, or used the SUBJECT ACCOUNT, including records about their identities and whereabouts.

ii. Information related to how and when the SUBJECT ACCOUNT was accessed or used;

iii. Any messages, records, documents, or material that identify the user(s) of the SUBJECT ACCOUNT.

iv. Information relating to the purchase, sale, distribution, transportation, possession and/or procurement of controlled substances, and the advertisement of controlled

substances for sale, including audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

v. Information relating to the proceeds of the sale or distribution of controlled substances, including the creation and use of bank, financial and cryptocurrency accounts, and records related to cryptocurrency, bank, and wire transactions;

vi. Messages, communications, audio recordings, pictures, video recordings, or still captured images relating to threats to commit acts of sexual or other physical violence against women or girls;

vii. Records, documents, programs, applications, or materials referring to or containing the personal identifying information of any individual other than the user of the SUBJECT ACCOUNT, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, and email addresses.

viii. Records, documents, programs, applications, or materials regarding any tax-related records, filings, or correspondence for any individual other than the user of the SUBJECT ACCOUNT.

ix. Information relating to the location, storage, or concealment of cash, money instruments, virtual currency, or money equivalents;

x. Information relating to co-conspirators engaged in the SUBJECT OFFENSES, which could include information relating to their identities, whereabouts, communications, and methods of contact and communication;

b. All records and information described above in Section II.10.b.

i. Any information identifying the device or devices used to access the SUBJECT ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifier, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC address, Electronic Serial Number ("ESN"), Mobile Electronic Identity Number ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Number ("MIN"), Subscriber Identity Module ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifier ("IMSI"), International Mobile Equipment Identity ("IMEI"), or Apple advertiser ID or ID for advertisers ("IDFA") or Google's AAID or any other advertiser ID, and any other information regarding the types of devices used to access the SUBJECT ACCOUNT or other device-specific information, including the device type, brand name, device mode or operating system, and first and last times that a device were observed;

IV. PROVIDER PROCEDURES

12. IT IS ORDERED that the PROVIDER shall deliver the information set forth in Section II within 10 days of the

service of this warrant. The PROVIDER shall send such information to:

Martina Doino

501 West Ocean Boulevard, suite 7200
Long Beach, California 90812
562-480-1569
Martina.doino@hsd.dhs.gov

13. IT IS FURTHER ORDERED that the PROVIDER shall provide the name and contact information for all employees who conduct the search and produce the records responsive to this warrant. IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 2705(b), that the PROVIDER shall not notify any person, including the subscriber(s) of each account identified in Attachment A, of the existence of the warrant, until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date this warrant is signed by the magistrate judge or such later date as may be set by the Court upon application for an extension by the United States. Upon expiration of this order, at least ten business days prior to disclosing the existence of the warrant, the PROVIDER shall notify the agent identified in paragraph 12 above of its intent to so notify.

AFFIDAVIT

I, Martina Doino, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security ("DHS"). Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), and have been so employed since December 2019. I am currently assigned to the HSI Office of the Special Agent in Charge in Los Angeles, California. I attended the HSI Criminal Investigator Training Program at the Federal Law Enforcement Training Center ("FLETC"), in Glynco, Georgia. At FLETC, I received training in conducting criminal investigations into narcotics smuggling, interdiction, and distribution of controlled substances.

2. I am currently assigned to the Los Angeles Border Enforcement Security Taskforce ("LA BEST") in Los Angeles, California, and have been so assigned since August 2021. LA BEST is a multiagency task force aimed at identifying, targeting, and eliminating vulnerabilities to the security of the United States related to the Los Angeles/Long Beach seaport complex, as well as the surrounding transportation and maritime corridors. My responsibilities include the investigation of violations of federal criminal laws, including crimes involving money laundering, narcotics trafficking, smuggling, fraud, and immigration violations.

3. Prior to my tenure as a special agent, I was a police officer in Key Biscayne, Florida from February 2015 to May 2019.

From July 2018 to May 2019, I was a Task Force Officer ("TFO") on a High Intensity Drug Trafficking Area Task Force, where I participated in investigations into money laundering and drug trafficking crimes in South Florida. Throughout my law enforcement career, I have participated in numerous criminal investigations involving narcotics importation, exportation or distribution. Through these investigations, I am familiar with the methods and practices of drug users, drug traffickers, and drug manufacturers. I have also spoken at length with other HSI SAs and local law enforcement officers regarding methods of drug trafficking.

4. During the course of my duties, I have become familiar with the manner in which controlled substances are packaged, marketed, and consumed. During the course of my current duties, I have become familiar with the ordinary meaning of controlled substance slang and jargon, and I am familiar with the manners and techniques of traffickers in controlled substances as practiced locally.

5. As a law enforcement officer, I have participated in numerous investigations involving drug trafficking organizations. Pursuant to my participation in those investigations, I have performed various tasks which include, but are not limited to: (a) functioning as a case agent, which entails the supervision of specific investigations involving the trafficking of drugs and the laundering of monetary instruments; (b) functioning as a surveillance agent and thereby observing and recording movements of persons trafficking in drugs and

those suspected of trafficking drugs; (c) interviewing witnesses, cooperating individuals, and informants relative to the illegal trafficking of drugs and the distribution of monies and assets derived from the illegal trafficking of drugs (laundering of monetary instruments); (d) participating in the tracing of monies and assets gained by drug traffickers from the illegal sale of drugs (laundering of monetary instruments); and (e) participating in investigations involving the purchase of controlled substances, the execution of search warrants, surveillance in connection with narcotic investigations, and the interview of confidential sources.

6. Through my investigations, my training and experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods employed by controlled substance traffickers to smuggle and safeguard controlled substances, distribute controlled substances, and collect and launder the proceeds from the sale of controlled substances. These methods include, but are not limited to, the use of wireless communications technology, such as cellular telephones and prepaid cellular accounts; counter surveillance; false or fictitious identities; and coded or vague communications in an attempt to avoid detection by law enforcement.

7. I make this affidavit in support of an application for a warrant for information associated with the account identified as arizonasewingworks@gmail.com (the "SUBJECT ACCOUNT") that is stored at premises controlled by Google, LLC (the "PROVIDER"), a

provider of electronic communication and remote computing services, headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.¹ The information to be searched is described in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. §§ 2703(a), 2703(b) (1) (A), 2703(c) (1) (A) and 2703(d)² to require the PROVIDER to disclose to the government copies of the information (including the content of communications) described in Section II of Attachment B. Upon receipt of the information described

¹ Because this Court has jurisdiction over the offense(s) being investigated, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. §§ 2703(a), (b) (1) (A), (c) (1) (A). See 18 U.S.C. §§ 2703(a) ("A governmental entity may require the disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction") and 2711 ("the term 'court of competent jurisdiction' includes -- (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that -- (i) has jurisdiction over the offense being investigated; (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title").

² The government is seeking non-content records pursuant to 18 U.S.C. § 2703(d). To obtain the basic subscriber information, which does not contain content, the government needs only a subpoena. See 18 U.S.C. § 2703(c) (1), (c) (2). To obtain additional records and other information--but not content--pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with the dictates of section 2703(c) (1) (B), which requires the government to supply specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation in order to obtain an order pursuant to 18 U.S.C. § 2703(d). The requested warrant calls for both records containing content (see Attachment B paragraph II.10.a.) as well as subscriber records and other records and information that do not contain content (see Attachment B paragraph II.10.b.).

in Section II of Attachment B, law enforcement agents and/or individuals assisting law enforcement and acting at their direction will review that information to locate the items described in Section III of Attachment B. Attachments A and B are incorporated herein by reference.

8. As described more fully below, I respectfully submit there is probable cause to believe that the information associated with the SUBJECT ACCOUNT constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of violations of 21 U.S.C. §§ 841 (possession with intent to distribute and distribution of controlled substances) and 846 (conspiracy to distribute controlled substances), 953 (exportation of controlled substances) (the "Subject Offenses").

9. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF PROBABLE CAUSE

10. On October 23, 2023, CBP inspected a consignment of a commercial manufacturing and shoe repair machine destined for Australia. CBP Officers discovered three packages containing approximately 32.78 kilograms of a substance that field tested

positive for methamphetamine concealed within the machine (defined below as the TARGET SHIPMENT).

11. HSI opened an investigation to determine the origin of the methamphetamine. The investigation revealed that an email identified as arizonasewingworks@gmail.com (the "SUBJECT ACCOUNT") arranged the transportation of the TARGET SHIPMENT.

III. STATEMENT OF PROBABLE CAUSE

12. I am aware of the following facts based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses.

13. According to my review of reports, on October 23, 2023, CBP Officers at the Long Beach port inspected the shipment with Internal Transaction Number (ITN) X20231010750422 destined for Australia (the "TARGET SHIPMENT"). According to the electronic export information, the TARGET SHIPMENT contained one Manufacturing and Repair Machine totaling 464 kilograms. CBP Officers discovered three plastic wrapped packages concealed within the Manufacturing and Repair Machine that contained a substance. A Gemini Thermo test determined the substance was positive for methamphetamine. In total, CBP Officers seized approximately 32.78 kilograms (including packaging weight) of the suspected methamphetamine.

14. The Automated Export System (AES) is a joint venture between the United States Federal Government and the export trade community. AES collects, processes, and stores shipment data, known as Electronic Export Information (EEI), for goods

exported from the United States. Some export shipments filed in AES require an ITN depending on the circumstances. I have reviewed the AES information for the TARGET SHIPMENT.

15. In export transactions, the Ultimate Consignee, or simply, Consignee, is the person or entity located abroad that is considered the owner of the goods for the purpose of customs declarations. Under Australian law, the Consignee is defined as the ultimate recipient of goods that have been sent from outside Australia, whether or not that person ordered or paid for the goods.

16. According to AES, the Consignee for the TARGET SHIPMENT was identified as "Ace Shoe Repairs" at Shop 5, 1003 Victoria Road, West Ryde in New South Wales 2114. The commercial invoice stated the email address for the Consignee was quoanh.to@outlook.com.

17. In export transactions, the U.S. Principal Party in Interest ("USPPI") is the person or legal entity in the United States that receives the primary benefits, monetary or otherwise, from an export transaction. Typically, the USPPI is the U.S. seller, manufacturer, or other party that received the order for the export of the goods.

18. According to AES, the USPPI for the TARGET SHIPMENT was identified as "Arizona Sewing Works" at 7217 East Pinnacle Pass Loop in Prescott, Arizona.

19. Based on publicly available information on the internet that I reviewed, "Arizona Sewing Works" was registered as a domestic non-profit corporation with the state of Arizona

in 2016. Arizona Sewing Works has been inactive, however, since approximately 2021.

20. In export transactions, the Forwarding Agent is person in the United States who is authorized by a USPPI to perform the services required to facilitate the export of goods from the United States.

21. According to AES, the Forwarding Agent for the TARGET SHIPMENT was identified as "Carotrans" at 100 Walnut Avenue in Clark, New Jersey 07066.

22. According to a series of email provided by Carotrans, that I reviewed, I am aware of the following:

a. a customer by the name of "Naomi Fraser" at email "Arizonasewingworks@gmail.com" (the "SUBJECT ACCOUNT") initiated the shipping process and hired Carotrans on or around October 9, 2023, as the freight forwarder for the TARGET SHIPMENT.

b. On October 9, 2023, the user of the SUBJECT ACCOUNT wrote, "Good morning, Team, Thank you for making contact regarding the above shipment order. I can confirm we are managing this. I will advise the we [sic] are organizing cartage on behalf of a paid fee from the client." The user of the SUBJECT ACCOUNT went on to sign the email, "Thank you, Naomi."

c. Email traffic shows the SUBJECT ACCOUNT communicated with Carotrans about the TARGET SHIPMENT numerous times between October 9 through October 25, 2023.

d. The SUBJECT ACCOUNT provided Carotrans with all requested documentation necessary to export the TARGET SHIPMENT.

e. The export documents provided to Carotrans such as the fumigation certificate and commercial invoice were signed by "Naomi Fraser".

23. Based on my knowledge of this investigation, my training, and my experience, I know it is common for international drug trafficking organizations to repeatedly use successful smuggling methods. I believe that "Naomi Fraser" is a fictitious individuals, and the SUBJECT ACCOUNT was created by the drug trafficking organization with the specific intent to facilitate narcotics smuggling while concealing the identities of the user. I believe that the contents of the SUBJECT ACCOUNT will aid in identifying the true users and other coconspirators involved in narcotics trafficking.

24. On approximately November 14, 2023, I sent the PROVIDER a preservation letter requesting that information associated with the SUBJECT ACCOUNT be preserved for 90 days pursuant to 18 U.S.C. § 2703(f).

25. Other than what has been described herein, to my knowledge the United States has not attempted to obtain the contents of the SUBJECT ACCOUNT by other means.

IV. BACKGROUND ON EMAIL AND SOCIAL MEDIA ACCOUNTS AND THE PROVIDER

26. In my training and experience, I have learned that providers of email and/or social media services offer a variety of online services to the public. Providers, like the PROVIDER, allow subscribers to obtain accounts like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with the provider.

During the registration process, providers generally ask their subscribers to provide certain personal identifying information when registering for an email or social media account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Some providers also maintain a record of changes that are made to the information provided in subscriber records, such as to any other email addresses or phone numbers supplied in subscriber records. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of an account.

27. Therefore, the computers of the PROVIDER are likely to contain stored electronic communications and information concerning subscribers and their use of the PROVIDER's services, such as account access information, email or message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

28. A subscriber of the PROVIDER can also store with the PROVIDER files in addition to emails or other messages, such as address books, contact or buddy lists, groups, social network links, calendar data, pictures or videos (other than ones attached to emails), notes, and other files, on servers

maintained and/or owned by the PROVIDER. In my training and experience, evidence of who was using an account may be found in such information.

29. In my training and experience, email and social media providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email and social media providers often have records of the Internet Protocol ("IP") address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a SUBJECT ACCOUNT.

30. In my training and experience, email and social media account users will sometimes communicate directly with the service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers of emails and social media services typically retain records about such communications, including records of contacts between the user and the provider's support services,

as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the user(s) of a SUBJECT ACCOUNT.

V. BACKGROUND ON THE SEIZURE OF DIGITAL EVIDENCE FROM THE PROVIDER

31. I know from my training and experience that the complete contents of an account may be important to establishing the actual user who has dominion and control of that account at a given time. Accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. Given the ease with which accounts may be created under aliases, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of an account, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular account. Only by piecing together information contained in the contents of an account may an investigator establish who the actual user of an account was. Often those pieces will come from a time period before the account was used in the criminal activity. Limiting the scope of the search would, in some instances, prevent the government from identifying the true user of the account and, in other instances, may not provide a defendant with sufficient information to identify other users of the account. Therefore, the contents of a given account,

including the email addresses or account identifiers and messages sent to that account, often provides important evidence regarding the actual user's dominion and control of that account. For the purpose of searching for content demonstrating the actual user(s) of a SUBJECT ACCOUNT, I am requesting a warrant requiring the PROVIDER to turn over all information associated with a SUBJECT ACCOUNT with the date restriction included in Attachment B for review by the search team.

32. Relatedly, the government must be allowed to determine whether other individuals had access to a SUBJECT ACCOUNT. If the government were constrained to review only a small subsection of an account, that small subsection might give the misleading impression that only a single user had access to the account.

33. I also know based on my training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or codewords (which require entire strings or series of conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and parenthesis :) to convey a smile or agreement) to discuss

matters. "Keyword searches" would not account for any of these possibilities, so actual review of the contents of an account by law enforcement personnel with information regarding the identified criminal activity, subject to the search procedures set forth in Attachment B, is necessary to find all relevant evidence within the account.

34. This application seeks a warrant to search all responsive records and information under the control of the PROVIDER, which is subject to the jurisdiction of this court, regardless of where the PROVIDER has chosen to store such information.

35. As set forth in Attachment B, I am requesting a warrant that permits the search team to keep the original production from the PROVIDER, under seal, until the investigation is completed and, if a case is brought, that case is completed through disposition, trial, appeal, or collateral proceeding.

a. I make that request because I believe it might be impossible for a provider to authenticate information taken from a SUBJECT ACCOUNT as its business record without the original production to examine. Even if the provider kept an original copy at the time of production (against which it could compare against the results of the search at the time of trial), the government cannot compel the provider to keep a copy for the entire pendency of the investigation and/or case. If the original production is destroyed, it may be impossible for the provider to examine a particular document found by the search

team and confirm that it was a business record of the provider taken from a SUBJECT ACCOUNT.

b. I also know from my training and experience that many accounts are purged as part of the ordinary course of business by providers. For example, if an account is not accessed within a specified time period, it -- and its contents -- may be deleted. As a consequence, there is a risk that the only record of the contents of an account might be the production that a provider makes to the government, for example, if a defendant is incarcerated and does not (perhaps cannot) access his or her account. Preserving evidence, therefore, would ensure that the government can satisfy its Brady obligations and give the defendant access to evidence that might be used in his or her defense.

VI. REQUEST FOR NON-DISCLOSURE

36. Pursuant to 18 U.S.C. § 2705(b), I request that the Court enter an order commanding the PROVIDER not to notify any person, including the subscriber(s) of the SUBJECT ACCOUNT, of the existence of the warrant until further order of the Court, until written notice is provided by the United States Attorney's Office that nondisclosure is no longer required, or until one year from the date the requested warrant is signed by the magistrate judge, or such later date as may be set by the Court upon application for an extension by the United States. There is reason to believe that such notification will result in flight from prosecution; destruction of or tampering with evidence; intimidation of potential witnesses; otherwise

seriously jeopardizing the investigation. The current investigation set forth above is not public, and I know, based on my training and experience, that drug traffickers often destroy digital evidence if they learn of an investigation. In addition, if the PROVIDER or other person notifies the targets of the investigation that a warrant has been issued for a SUBJECT ACCOUNT, the unidentified subjects might further mask their activity and seriously jeopardize the investigation.

VII. CONCLUSION

37. Based on the foregoing, I request that the Court issue the requested warrant. The government will execute this warrant by serving the warrant on the PROVIDER. Because the warrant will be served on the PROVIDER, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ____ day of December 2023.

UNITED STATES MAGISTRATE JUDGE